МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

Першого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

Кваліфікація: Бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ ЦНТУ
Протокол № 8 від 24 04 2017р.

Освітня програма вводиться в дію
з 1.09 2017р.
Ректор _____М.І.Черновол

Кропивницький 2017

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

Рівень вищої освіти	**Перший (бакалаврський)**
ГАЛУЗЬ ЗНАНЬ	**12 Інформаційні технології**
СПЕЦІАЛЬНІСТЬ	**125 Кібербезпека**
КВАЛІФІКАЦІЯ	**Бакалавр з кібербезпеки**

РОЗРОБЛЕНО І СХВАЛЕНО
Науково-методичною комісією
спеціальності 123
Комп'ютерна інженерія

Протокол № 2
від «27» 03 2017 р.
Голова НМК спеціальності

_____О.А.Смірнов

ПОГОДЖЕНО
Перший проректор
Центральноукраїнського
національного технічного
університету

_____ В.М. Кропівний
«24» 04 2017 р.

РЕКОМЕНДОВАНО
Науково-методичною радою
університету
Протокол № 8
від «17» 04 2017 р.
Голова НМР університету

_____ В.М. Кропівний

Ректор
Центральноукраїнського
національного технічного
університету

_____ М.І. Черновол
«24» 04 2017 р.

ПЕРЕДМОВА

Розроблено робочою групою (науково-методичною комісією) спеціальності 123 Комп’ютерна інженерія у складі:
1. Мелешко Єлизавета Владиславівна, к.т.н., доц., доцент кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
2. Смірнов Олексій Анатолійович, д.т.н., проф., професор кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
3. Сидоренко Володимир Володимирович, д.т.н., проф., професор кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
4. Минайленко Роман Миколайович, к.т.н., доц.., доцент кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
5. Коваленко Анна Степанівна, к.т.н., старший викладач кафедри кібербезпеки та програмного забезпечення, ЦНТУ.
6. Лисенко Ірина Анатоліївна, к.т.н., старший викладач кафедри кібербезпеки та програмного забезпечення, ЦНТУ.

1. Профіль освітньої програми «Кібербезпека»
зі спеціальності 125 «Кібербезпека»

1. Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	Центральноукраїнський національний технічний університет, механіко-технологічний факультет, кафедра кібербезпеки та програмного забезпечення
Ступінь вищої освіти та назва кваліфікації	Бакалавр з кібербезпеки, фахівець із організації інформаційної безпеки
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання – 3 роки 10 місяців
Наявність акредитації	
Цикл/рівень	Національна рамка кваліфікацій України (6 рівень, другий магістерський рівень) Рамка кваліфікацій Європейського простору вищої освіти QF EHEA (1st cycle) Європейська рамка кваліфікацій для навчання впродовж життя EQF LLL (level 6)
Передумови	Повна загальна середня освіта
Мова(и) викладання	Українська, англійська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення опису освітньої програми	http://it-kntu.kr.ua/ http://dspace.kntu.kr.ua/

2. Мета освітньої програми	
Забезпечити підготовку висококваліфікованих фахівців в галузі інформаційних технологій зі спеціальності 125 «Кібербезпека», здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього кібернетичного впливу, здатних розробляти і використовувати технології інформаційної безпеки.	
3. Характеристика освітньої програми	
Предметна область	Галузь знань – 12 «Інформаційні технології» («Information technologies») Спеціальність – 125 «Кібербезпека» («Cyber Security»)
Орієнтація освітньої програми	Освітньо-професійна програма . Ступінь освіти – бакалавр.
Фокус програми	Здобуття вищої освіти в галузі інформаційні технології, спеціальності «Кібербезпека». Акцент на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.
Особливості програми	Інтеграція програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності.
4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівець може працювати в підрозділах великих підприємств та установ, забезпечуючи захист комп'ютерних систем та мереж, у відділах спецслужб та правозахисних органів для захисту кіберпростору та інформаційних даних, здійснювати забезпечення захищеної комп'ютеризованої діяльності банків та фінансових установ, виконувати функції розробника

	систем захисту інформації Фахівець може займати первинні посади (за ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки. International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
Подальше навчання	Право продовження освіти на другому (магістерському) рівні.
5. Викладання та оцінювання	
Викладання та навчання	Втілення в освітньому процесі студентоцентричного підходу; нерозривності процесів навчання і наукових досліджень; забезпечення гарантованої якості освіти відповідно до стандартів освіти; врахування світового досвіду, потреб ринку праці, залучення до цього процесу роботодавців, провідних учених, фахівців-практиків, випускників і здобувачів вищої освіти; впровадження інноваційних навчальних технологій; забезпечення здобувачам вищої освіти сприятливих умов для самостійного навчання та творчого розвитку; інтеграція освітньої та наукової діяльності; забезпечення зворотних зв'язків між учасниками освітнього процесу.
Оцінювання	*Види контролю*: поточний, тематичний, періодичний, підсумковий, самоконтроль. *Форми контролю*: усне та письмове опитування, тестовий контроль, захист лабораторних та індивідуальних робіт, підсумкова атестація – захист бакалаврської роботи

6. Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
	КЗ 2. Знання та розуміння предметної області та розуміння професії.
	КЗ 3. Здатність спілкуватися рідною та другою іноземною мовою як усно, так і письмово
	КЗ 4. Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки
	КЗ 5. Вміння виявляти, ставити та вирішувати проблеми.
	КЗ 6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
	КЗ 7. Навички міжособистісної взаємодії.
	КЗ 8.Прагнення до збереження навколишнього середовища
	КЗ 9. Здатність діяти соціально відповідально та громадянсько свідомо.
	КЗ 10. Здатність вчитися і бути сучасно навченим.
	КЗ 11. Здатність приймати обґрунтовані рішення.
	КЗ 12. Здатність до адаптації та дії в новій ситуації.
	КЗ 13. Дотримання та пропагування здорового способу життя.
	КЗ 14. Здатність бути критичним та самокритичним
Фахові компетентності	КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.
	КФ 2. Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС, каналів зв'язку, систем управління процесами, баз даних, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації.
	КФ 3. Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки
	КФ 4. Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі
	КФ 5Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем
	КФ 6. Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов
	КФ 7. Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС
	КФ 8. Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки

	КФ 9. Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою
	КФ 10. Здатність здійснювати управління інцидентами інформаційної та кібербезпеки
	КФ 11. Здатність здійснювати управління ризиками інформаційної та кібербезпеки
	КФ 12. Здатність виконувати моніторинг даних, комп'ютерних зловживань та аномалій
	КФ 13. Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники
	КФ 14. Здатність проводити дослідження у практичній професійній діяльності
7. Програмні результати навчання	
	Загальні результати навчання
	- застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки;
	- проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави,а також напрямків розвитку інформаційної та кібербезпеки;
	-застосувати знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації;
	- дотримуватись вимог санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки при здійсненні професійної діяльності;
	організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність;
	-використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
	-дотримуватись норм міжособистісного спілкування у професійній взаємодії;
	-прогнозувати наслідки результатів діяльності людини з метою збереження навколишнього середовища;
	-використовувати історичну спадщину та культурні традиції свого народу для професійного зростання, саморозвитку, самовдосконалення;
	-вдосконалювати професійний та особистісний розвиток протягом усього життя;
	- аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності,які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
	-адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

	-демонструвати та пропагуватиздоровий спосіб життя;
	- критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
	Фахові результати навчання
	діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; - готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки;
	– здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; – застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; – використати спеціалізовані комп'ютерні програми в професійній діяльності. – обирати відповідну технологію програмування, виконати аналіз специфікації задач; – виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування;
	– виконувати декомпозицію ІТС; – розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; - розробляти модель загроз, розробляти модель порушника; - розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; – вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; – вибирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; – проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації;
	– застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах;
	– здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; – здійснювати оцінку захищеності ІТ систем та мереж; – використовувати інструментальні засоби оцінки наявних вразливостей; – оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж;
	– виконувати налаштування інформаційних систем та комунікаційного обладнання;

	– виконувати захист інформаційних систем від комп'ютерних вірусів; – забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; – організовувати процес створення планів неперервності бізнесу; – приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ;
	– виявляти небезпечні сигнали технічних засобів; – вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту інформації – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах – виконувати дослідження, перевірку, аналіз та оцінювання об'єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації
	– обґрунтування інвестицій в інформаційну безпеку; – аналізувати економічну ефективність заходів інформаційної безпеки; – визначати особливості організаційної структури та організації робіт; – використовувати міжнародні та національні специфічні для сектора економіки вимоги та кращі практики;
	– приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; – приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки; – на основі політики захисту організації розробляти нормативні документи для її реалізації;
	– впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; – застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцендентів інформаційної безпеки;
	– розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем – застосовувати політики, що базуються риск адаптивному контролі доступу – здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та

	загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками
	– виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС. – використовувати інструментарій для моніторингу даних в ІТС. – виконувати аналіз зловмисного програмного коду
	– характеризувати стан інформаційної безпеки особистості, суспільства та держави; – характеризувати основні форми інформаційного протиборства в умовах входження держави в інформаційне суспільство;
	– використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; – застосовувати системний підхід та знання основ теорії інформаційної безпеки.
8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Лекції проводяться науково-педагогічними працівниками, а також провідними науковцями або спеціалістами практиками (включаючи фахівців іноземних країн), запрошеними для читання лекцій.
Матеріально-технічне забезпечення	Забезпечення комп'ютерною технікою та технологіями сучасного рівня
Інформаційне та навчально-методичне забезпечення	Доступ до найсучасніших інформаційних технологій та ресурсів
9. Академічна мобільність	
Навчання іноземних здобувачів вищої освіти	Мовою викладання в ЦНТУ є державна мова. З метою створення умов для міжнародної академічної мобільності, ЦНТУ має право приймати рішення про викладання однієї чи кількох дисциплін англійською мовою чи іншою офіційною мовою Європейського Союзу, забезпечивши при цьому знання здобувачами вищої освіти з відповідної дисципліни державною мовою. Перелік іноземних мов, якими здійснюється викладання навчальних дисциплін, визначається ЦНТУ. Для викладання навчальних дисциплін іноземною мовою ЦНТУ може утворювати окремі групи для іноземних громадян, осіб без громадянства, які бажають здобувати вищу освіту, за кошти фізичних чи юридичних осіб, або розробляти індивідуальні програми. При цьому ЦНТУ забезпечує вивчення такими особами державної мови як окремої навчальної дисципліни.

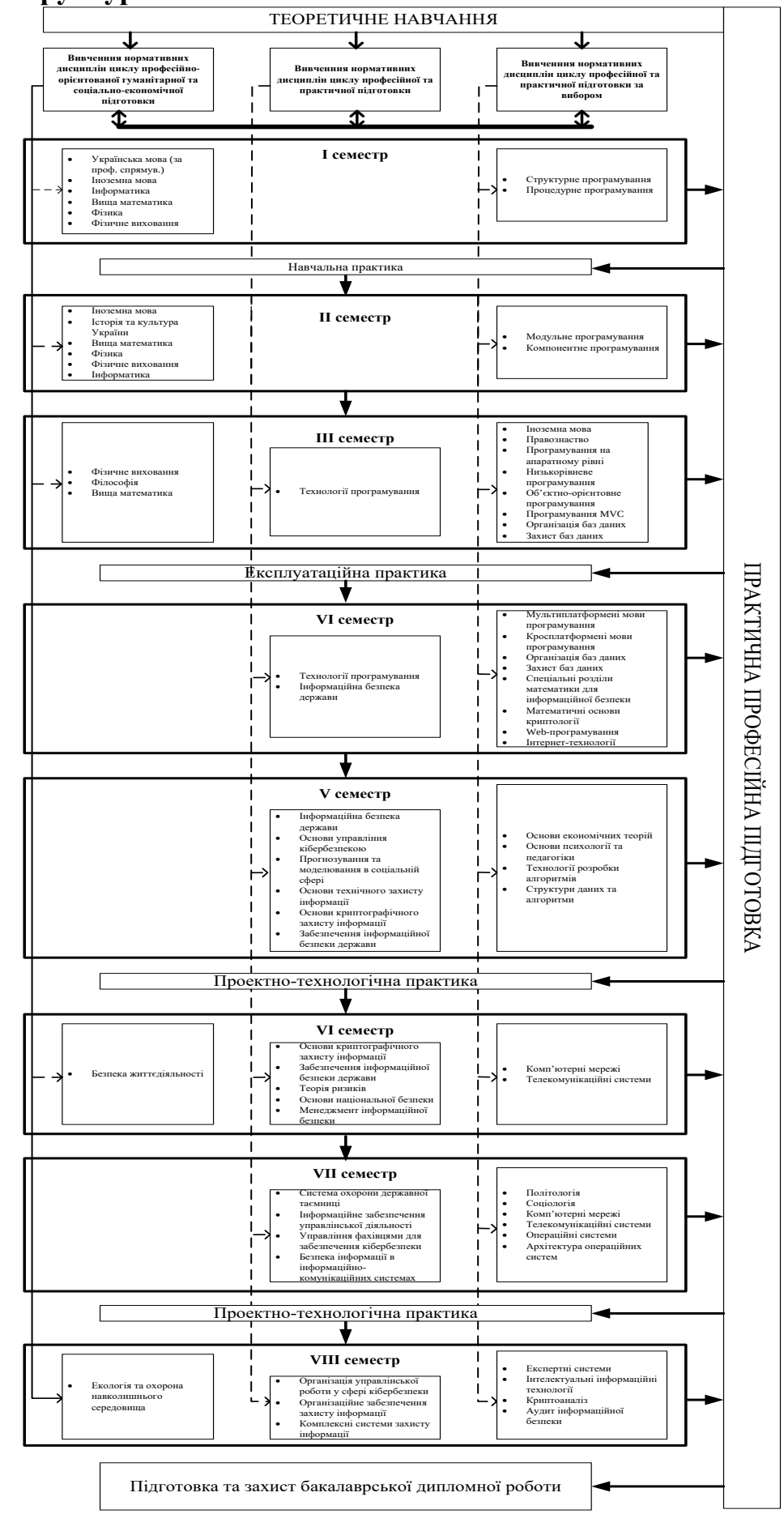
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

	Компоненти освітньої програми	Кільк. кред.	Форма підсумк. контр.
	Обов'язкові компоненти		
1.	Українська мова (за проф. спрямув.)	3	екзамен
2.	Іноземна мова	5	залік, екзамен
3.	Історія та культура України	5	екзамен
4.	Фізика	9	залік, екзамен
5.	Інформатика	9	екзамен
6.	Фізичне виховання	6	залік
7.	Вища математика	16	екзамен
8.	Філософія	4	екзамен
9.	Безпека життєдіяльності	2	залік
10.	Екологія та охорона навколишнього середовища	3	залік
11.	Технології програмування	8	екзамен
12.	Інформаційна безпека держави	8	залік, екзамен
13.	Основи управління кібербезпекою	4	екзамен
14.	Прогнозування та моделювання в соціальній сфері	5	екзамен
15.	Основи технічного захисту інформації	4	екзамен
16.	Основи криптографічного захисту інформації	7	залік, екзамен
17.	Забезпечення інформаційної безпеки держави	7	залік, екзамен
18.	Теорія ризиків	3	екзамен
19.	Основи національної безпеки	4	екзамен
20.	Система охорони державної таємниці	3	залік
21.	Інформаційне забезпечення управлінської діяльності	4	екзамен

22.	Менеджмент інформаційної безпеки	5	екзамен
23.	Управління фахівцями для забезпечення кібербезпеки	4	екзамен
24.	Безпека інформації в інформаційно-комунікаційних системах	4	екзамен
25.	Організація управлінської роботи у сфері кібербезпеки	3	екзамен
26.	Організаційне забезпечення захисту інформації	3	екзамен
27.	Комплексні системи захисту інформації	4	екзамен
28.	Навчальна практика	6	диф.залік
29.	Експлуатаційна практика	6	диф.залік
30.	Проектно-технологічна практика	6	диф.залік
31.	Переддипломна практика	6	диф.залік
32.	Дипломне проектування	9	
	Загальний обсяг обов'язкових компонент	169	
	Вибіркові компоненти		
1.	Іноземна мова	3	залік
2.	Правознавство	3	залік
3.	Основи економічних теорій	3	залік
4.	Основи психології та педагогіки	3	залік
5.	Політологія	3	залік
6.	Соціологія	3	залік
7.	Структурне програмування	5	екзамен
8.	Процедурне програмування	5	екзамен
9.	Модульне програмування	6	екзамен
10.	Компонентне програмування	6	екзамен
11.	Програмування на апаратному рівні	4	екзамен
12.	Низькорівневе програмування	4	екзамен
13.	Об'єктно-орієнтоване програмування	5	екзамен
14.	Програмування MVC	5	екзамен
15.	Організація баз даних	6	залік, екзамен

16.	Захист баз даних	6	залік, екзамен
17.	Мультиплатформені мови програмування	4	екзамен
18.	Кросплатформені мови програмування	4	екзамен
19.	Спеціальні розділи математики для інформаційної безпеки	7	екзамен
20.	Математичні основи криптології	7	екзамен
21.	Web-програмування	5	екзамен
22.	Інтернет-технології	5	екзамен
23.	Технології розробки алгоритмів	4	екзамен
24.	Структури даних та алгоритми	4	екзамен
25.	Комп'ютерні мережі	7	залік, екзамен
26.	Телекомунікаційні системи	7	залік, екзамен
27.	Операційні системи	3	екзамен
28.	Архітектура операційних систем	3	екзамен
29.	Експертні системи	3	екзамен
30.	Інтелектуальні інформаційні технології	3	екзамен
31.	Криптоаналіз	3	екзамен
32.	Аудит інформаційної безпеки	3	екзамен
	Загальний обсяг вибіркових компонент	**71**	
	Загальний обсяг освітньої програми	**240**	

Структурно-логічна схема ОП



3. Форми атестації здобувачів вищої освіти

Атестацією здобувачів вищої освіти першого (бакалаврського) рівня освітньої програми «Кібербезпека» є публічний захист (демонстрація) кваліфікаційної роботи - бакалаврської роботи.

В процесі публічного захисту претендент ступеня бакалавра повинен показати уміння чітко і упевнено викладати зміст виконаних досліджень, аргументовано відповідати на запитання і вести дискусію.
Доповідь студента повинна супроводжуватися презентаційними матеріалами та пояснювальною запискою, призначеними для загального перегляду.
Ухвалення екзаменаційною комісією рішення про присудження ступеня бакалавра з кібербезпеки та видачу диплома бакалавра за результатами підсумкової атестації студентів оголошуються того самого дня після оформлення в установленому порядку протоколів засідань екзаменаційної комісії.
Атестація завершується видачею документу встановленого державного зразка про присудження ступеня бакалавра із присвоєнням кваліфікації: «Бакалавр з кібербезпеки».

4. Відповідність компетентностей і результатів навчання

Загальні компетентності	Результати навчання
КЗ 1. Здатність застосовувати знання у практичних ситуаціях (*Здатність до застосування концептуальних знань та певних знань сучасних досягнень у професійній діяльності)*	- застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки;
КЗ 2. Знання та розуміння предметної області та розуміння професії. (*Здатність розуміти сутність та соціальну значущість майбутньої професійної діяльності, виявляти стійкий інтерес до неї)*	- проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави,а також напрямків розвитку інформаційної та кібербезпеки;
КЗ 3. Здатність спілкуватися рідною та другою мовою як усно, так і письмово (*Здатність до усної та письмової ділової комунікації державною мовою та однією з іноземних мов*)	-застосувати знання державної та однієї з іноземних мов з метою забезпечення ефективності професійної комунікації;
КЗ 4. Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки	- дотримуватись вимог санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки при здійсненні професійної діяльності;
КЗ 5. Вміння виявляти, ставити та вирішувати проблеми. *(Здатність раціонально організовувати власну професійну діяльність, обирати методи та способи розв'язання складних спеціалізованих задач та практичних проблеми в професійній фармацевтичній діяльності, оцінювати їхню ефективність).*	організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність;
КЗ 6. Здатність до пошуку, обробки та аналізу інформації з різних джерел. (*Здатність до самостійного пошуку, аналізу, синтезу та використання інформації, необхідної для ефективного розв'язання професійних завдань*.)	-використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
КЗ 7. Навички міжособистісної взаємодії. *(Здатність до ефективної міжособистісної та командної взаємодії в професійній та соціальній діяльності).*	-дотримуватись норм міжособистісного спілкування у професійній взаємодії;
КЗ 8.Прагнення до збереження навколишнього середовища (*Здатність розуміти наслідки діяльності людини для природного та соціального середовища*).	-прогнозувати наслідки результатів діяльності людини з метою збереження навколишнього середовища;
КЗ9. Здатність діяти соціально відповідально та громадсько свідомо *(Здатність діяти соціально відповідально та громадсько свідомо з урахуванням історичної спадщини та культурних традицій свого народу)*	-використовувати історичну спадщину та культурні традиції свого народу для професійного зростання, саморозвитку, самовдосконалення;
КЗ 10. Здатність вчитися і бути сучасно навченим *(Здатність визначати завдання*	-вдосконалювати професійний та особистісний розвиток протягом усього

професійного та особистісного розвитку протягом усього життя, здійснювати самоосвіту, самовдосконалення, підвищення кваліфікації).	життя;
КЗ 11. Здатність приймати обґрунтовані рішення. *(Здатність приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, що характеризуються комплексністю та неповною визначеністю умов, нести за них відповідальність)*	- аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності,які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
КЗ 12. Здатність до адаптації та дії в новій ситуації. (*Здатність адаптуватися в соціальному та професійному середовищі*.)	-адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
КЗ 13. Дотримання та пропагування здорового способу життя.	-демонструвати та пропагуватиздоровий спосіб життя;
КЗ 14. Здатність бути критичним та самокритичним	Осмислювати критично основні теорії, принципи, методи і поняття у навчанні та професійній діяльності

Фахові компетентності	Результати навчання
КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних,стандартів та практик щодо здійснення професійної діяльності	– діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; – готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки;
КФ 2. Здатність до використання інформаційних і комунікаційних технологій	– здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; – застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; – використати спеціалізовані комп'ютерні програми в професійній діяльності. – Обирати відповідну технологію програмування, виконати аналіз специфікації задач; – виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування;
КФ 3. Здатність здійснювати проектування (розробку) систем, технологій і засобів кібербезпеки	– виконувати декомпозицію ІТС; – розробляти структурні схеми з відображенням зв'язків між інформаційними процесами на віддалених системах; – розробляти модель загроз, розробляти модель порушника; – розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; – вирішувати завдання захисту програм та даних ІТС програмно-апаратними засобами

	та давати оцінку якості прийнятих рішень; – обирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; – проектувати та реалізувати комплексні систему захисту інформації АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації;
КФ 4. Здатність здійснювати протидію несанкціонованому проникненню в ІТ системи і мережі	– застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційних і комунікаційних системах та мережах;
КФ 5. Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем	– здійснювати оцінку можливості проникнення в ІТ системи та мережі шляхом експлуатації наявних вразливостей; – здійснювати оцінку захищеності ІТ систем та мереж; – використовувати інструментальні засоби оцінки наявних вразливостей; – оцінювати можливості та ефективність застосування, в тих чи інших умовах, інструментальних засобів оцінки вразливостей ІТ систем та мереж;
КФ 6. Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов	– виконувати налаштування інформаційних систем та комунікаційного обладнання; – виконувати захист інформаційних систем від комп’ютерних вірусів; – забезпечувати впровадження та дотримання політики кіберзахисту в ІТС, процедур, і правил; – організовувати процес створення планів неперервності бізнесу; – приймати участь у розробці планів відновлення, неперервності процесів організації для забезпечення здатності організації продовжувати виконувати необхідну діяльність в період порушення ІТ;
КФ 7. Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС	– виявляти небезпечні сигнали технічних засобів; – вимірювати параметри небезпечних сигналів для технічних каналів витоку інформації та визначати ефективність захисту від витоку інформації відповідно до вимог нормативних документів системи технічного захисту інформації – інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТСМ відповідно до вимог нормативних документів системи технічного захисту

	інформації – проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах – виконувати дослідження, перевірку, аналіз та оцінювання об'єктів щодо їх відповідності вимогам нормативних документів та можливості їх використання для забезпечення інформації
КФ 8. Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки	– обґрунтування інвестицій в інформаційну безпеку; – аналізувати економічну ефективність заходів інформаційної безпеки; – визначати особливості організаційної структури та організації робіт; – використовувати міжнародні та національні специфічні для сектора економіки вимоги та кращі практики;
КФ 9. Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою	– приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; – приймати участь у розробці та впровадженні політики, стандартів та процедур інформаційної безпеки та/ або кібербезпеки; – на основі політики захисту організації розробляти нормативні документи для її реалізації;
КФ 10. Здатність здійснювати управління інцидентами інформаційної та кібербезпеки	– впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної/кібербезпеки; – застосовувати національні та міжнародні регулюючі актів в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцендентів інформаційної безпеки;
КФ 11. Здатність здійснювати управління ризиками інформаційної та кібербезпеки	– розробляти та оцінювати моделі і політику безпеки на основі використання сучасних принципів, способів та методів теорії захищених систем – застосовувати політики, що базуються риск адаптивному контролі доступу – здійснювати аналіз ризиків функціонування ІКС: визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювання та управління ризиками
КФ 12. Здатність виконувати моніторинг даних та виявлення комп’ютерних зловживань та аномалій	– виконувати конфігурування систем виявлення вторгнень та використовувати компоненти захисту для забезпечення необхідного рівня захищеності ІТС.

	– використовувати інструментарій для моніторингу даних в ІТС. – виконувати аналіз зловмисного програмного коду
КФ 13. Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники	– характеризувати стан інформаційної безпеки особистості, суспільства та держави; – характеризувати основні форми інформаційного протиборства в умовах входження держави в інформаційне суспільство;
КФ 14. Здатність проводити дослідження у практичній професійній діяльності на відповідному рівні	– використовувати теоретичні і практичні методи та методики досліджень у галузі інформаційної безпеки; – застосовувати системний підхід та знання основ теорії інформаційної безпеки.

5. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

Забезпечення якості підготовки здобувачів вищої освіти першого (бакалаврського) рівня освітньої програми «Кібербезпека» передбачає здійснення таких процедур і заходів:

- здійснення моніторингу та періодичного перегляду освітніх програм;
- щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті вищого навчального закладу, на інформаційних стендах та в будь-який інший спосіб;
- забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;
- забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;
- забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
- забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;
- забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників вищих навчальних закладів і здобувачів вищої освіти;
- інших процедур і заходів.